

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-083233
 (43)Date of publication of application : 21.03.2000

(51)Int.Cl.

H04N 7/16
 G06F 13/00
 H04H 1/00
 H04L 9/32
 H04N 5/91
 H04N 5/93
 H04N 7/24
 H04N 7/173

(21)Application number : 10-295936
 (22)Date of filing : 16.10.1998

(71)Applicant : CANON INC
 (72)Inventor : INOUE YUJI
 NAKAGAWA TOSHIYUKI

(30)Priority

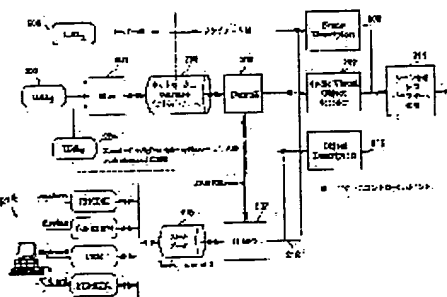
Priority number : 10183034 Priority date : 29.06.1998 Priority country : JP

(54) AUTHENTICATION DEVICE AND METHOD AND SYSTEM THEREFOR AND STORAGE MEDIUM

(57)Abstract

PROBLEM TO BE SOLVED: To attain the valid protection of copyrights and the valid use of a work by comparing authorization information included in received moving image data with inputted characters and symbols, and transmitting an instruction signal for instructing the re-reproduction of moving image data from reproduced initial image data to an outside information processor.

SOLUTION: A client divides a received MPEG-4 bit stream 205 into plural streams such as plural objects or the information of URL accompanying the objects by a demultiplexer 206. In this case, the information of the URL accompanying each object is transmitted to an IPMPS 207, and any URL information is selected, and an authentication request signal is transmitted to a multiplexer 201 having the corresponding URL connected on a network. When an access permission signal is received from the multiplexer 201, an access can be performed to an object whose access permission is obtained.



LEGAL STATUS

[Date of request for examination] 29.09.2005
 [Date of sending the examiner's decision of rejection]
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]
 [Patent number]
 [Date of registration]
 [Number of appeal against examiner's decision of rejection]
 [Date of requesting appeal against examiner's decision of rejection]
 [Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-83233
(P2000-83233A)

(43) 公開日 平成12年3月21日 (2000.3.21)

(51) Int.Cl. ¹	識別記号	F I	テーマコード* (参考)
H 0 4 N 7/16		H 0 4 N 7/16	Z
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z
H 0 4 H 1/00		H 0 4 H 1/00	Z
H 0 4 L 9/32		H 0 4 N 7/173	6 1 0 Z
H 0 4 N 5/91		H 0 4 L 9/00	6 7 5 A

審査請求 未請求 請求項の数34 O L (全 24 頁) 最終頁に続く

(21) 出願番号 特願平10-295936

(22) 出願日 平成10年10月16日 (1998. 10. 16)

(31) 優先権主張番号 特願平10-183034

(32) 優先日 平成10年6月29日 (1998. 6. 29)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 井上 裕司

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

(72) 発明者 中川 利之

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

(74) 代理人 100076428

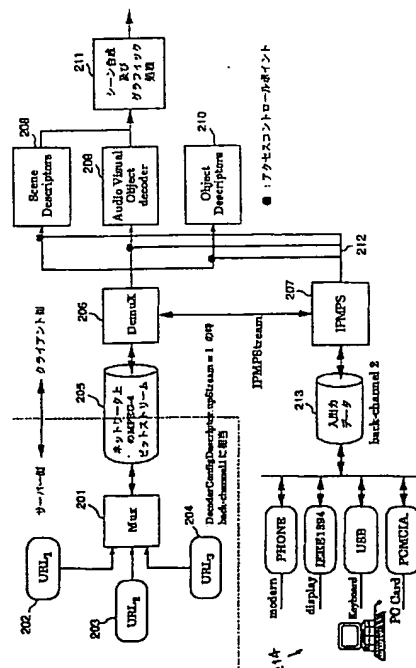
弁理士 大塚 康徳 (外2名)

(54) 【発明の名称】 認証装置及び認証方法及び認証システム並びに記憶媒体

(57) 【要約】

【課題】 オブジェクトの集合で構成される動画を再生するシステムにおいて、各オブジェクトの認証を効率的に行うとともに、認証処理に関わる遅延時間により再生映像が欠落する問題を解消する。

【解決手段】 オブジェクトの再送を要求する信号を、その要求先のサーバの出所情報と、認証結果を示す情報とともに、back-channel 1 (205) 又は2 (213) を使用して、認証を要求するオブジェクトの配信サーバ (202~204) へと送信する。



【特許請求の範囲】

【請求項1】 外部情報処理装置より利用許可情報を含む動画像データを受信する受信手段と、

前記受信手段により受信された動画像データの一部を再生する再生手段と、

文字・記号を入力する入力手段と、前記受信手段により受信された動画像データに含まれる利用許可情報と、前記入力手段により入力された文字・記号とを比較する比較手段と、前記比較手段による比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生手段により再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記外部情報処理装置へと送信する送信手段とを具備したことを特徴とする認証装置。

【請求項2】 前記動画像データは、圧縮符号化された動画像データであることを特徴とする請求項1に記載の認証装置。

【請求項3】 前記文字・記号をあらかじめ記憶した記憶手段を有し、前記比較手段は、前記受信手段により受信された動画像データに含まれる利用許可情報と、前記記憶手段に記憶された文字・記号とを比較することを特徴とする請求項1に記載の認証装置。

【請求項4】 前記再生手段は、前記動画像データの時間的一部分若しくは空間的一部分を再生することを特徴とする請求項1に記載の認証装置。

【請求項5】 前記送信手段は、前記指示信号と共に、当該認証装置が前記動画像データを利用可能であることを示す信号を送信することを特徴とする請求項1に記載の認証装置。

【請求項6】 前記送信手段は、通常、前記動画像データの受信用に使用されるインターフェースを、通常の方法に使用して前記動画像データを受信する他、通常の方法と逆方向に使用して前記指示信号を送信することを特徴とする請求項1に記載の認証装置。

【請求項7】 前記送信手段は、MPEG4のビットストリームのアップストリームを使用して、前記指示信号を送信することを特徴とする請求項1に記載の認証装置。

【請求項8】 通信回線と接続するインターフェースを更に具備し、前記送信手段は、前記インターフェース及び前記通信回線を介して、前記指示信号を送信することを特徴とする請求項1に記載の認証装置。

【請求項9】 出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信手段と、前記受信手段により受信された動画像データを前記複数のオブジェクトデータの各々に分離する分離手段と、前記分離手段により分離されたオブジェクトデータのうち、利用許可情報を含まないオブジェクトデータを再生する再生手段と、文字・記号を入力する入力手段と、前記分離手段に

より分離されたオブジェクトデータのうち、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、前記入力手段により入力された文字・記号とを比較する比較手段と、前記比較手段による比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生手段により再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する外部情報処理装置へと送信する送信手段とを具備したことを特徴とする認証装置。

【請求項10】 前記出所情報は、URL (Uniform Resource Locator) の情報であることを特徴とする請求項9に記載の認証装置。

【請求項11】 外部情報処理方法より利用許可情報を含む動画像データを受信する受信ステップと、前記受信ステップにより受信された動画像データの一部を再生する再生ステップと、

文字・記号を入力する入力ステップと、前記受信ステップにより受信された動画像データに含まれる利用許可情報と、前記入力ステップにより入力された文字・記号とを比較する比較ステップと、前記比較ステップによる比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生ステップにより再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記外部情報処理方法へと送信する送信ステップとを具備したことを特徴とする認証方法。

【請求項12】 前記動画像データは、圧縮符号化された動画像データであることを特徴とする請求項11に記載の認証方法。

【請求項13】 前記文字・記号をあらかじめ記憶した記憶ステップを有し、前記比較ステップは、前記受信ステップにより受信された動画像データに含まれる利用許可情報と、前記記憶ステップに記憶された文字・記号とを比較することを特徴とする請求項11に記載の認証方法。

【請求項14】 前記再生ステップは、前記動画像データの時間的一部分若しくは空間的一部分を再生することを特徴とする請求項11に記載の認証方法。

【請求項15】 前記送信ステップは、前記指示信号と共に、当該認証方法が前記動画像データを利用可能であることを示す信号を送信することを特徴とする請求項11に記載の認証方法。

【請求項16】 前記送信ステップは、通常、前記動画像データの受信用に使用されるインターフェースを、通常の方法に使用して前記動画像データを受信する他、通常の方法と逆方向に使用して前記指示信号を送信することを特徴とする請求項11に記載の認証方法。

【請求項17】 前記送信ステップは、MPEG4のビ

ットストリームのアップストリームを使用して、前記指示信号を送信することを特徴とする請求項 11 に記載の認証方法。

【請求項 18】 通信回線と接続するインターフェースを更に具備し、前記送信ステップは、前記インターフェース及び前記通信回線を介して、前記指示信号を送信することを特徴とする請求項 11 に記載の認証方法。

【請求項 19】 出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信ステップと、前記受信ステップにより受信された動画像データを前記複数のオブジェクトデータの各々に分離する分離ステップと、前記分離ステップにより分離されたオブジェクトデータのうちの、利用許可情報を含まないオブジェクトデータを再生する再生ステップと、文字・記号を入力する入力ステップと、前記分離ステップにより分離されたオブジェクトデータのうちの、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、前記入力ステップにより入力された文字・記号とを比較する比較ステップと、前記比較ステップによる比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生ステップにより再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する外部情報処理方法へと送信する送信ステップとを具備したことを特徴とする認証方法。

【請求項 20】 前記出所情報は、URL (Uniform Resource Locator) の情報であることを特徴とする請求項 19 に記載の認証方法。

【請求項 21】 互いに通信可能に接続された情報処理装置と認証装置とを有する認証システムであって、前記認証装置が、前記情報処理装置から利用許可情報を含む動画像データを受信する受信手段と、前記受信手段により受信された動画像データの一部を再生する再生手段と、文字・記号を入力する入力手段と、前記受信手段により受信された動画像データに含まれる利用許可情報と、前記入力手段により入力された文字・記号とを比較する比較手段と、前記比較手段による比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生手段により再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記情報処理装置へと送信する送信手段とを具備したことを特徴とする認証システム。

【請求項 22】 少なくとも 1 つの情報処理装置と、該情報処理装置と互いに通信可能に接続された認証装置と

を有する認証システムであって、前記認証装置が、前記情報処理装置から出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信手段と、前記受信手段により受信された動画像データを前記複数のオブジェクトデータの各々に分離する分離手段と、前記分離手段により分離されたオブジェクトデータのうちの、利用許可情報を含まないオブジェクトデータを再生する再生手段と、文字・記号を入力する入力手段と、前記分離手段により分離されたオブジェクトデータのうちの、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、前記入力手段により入力された文字・記号とを比較する比較手段と、前記比較手段による比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生手段により再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する前記情報処理装置へと送信する送信手段とを具備したことを特徴とする認証システム。

【請求項 23】 装置が実行可能なプログラムを格納する記憶媒体であって、前記プログラムを実行する装置を、外部情報処理装置より利用許可情報を含む動画像データを受信する受信手段と、前記受信手段により受信された動画像データの一部を再生する再生手段と、文字・記号を入力する入力手段と、前記受信手段により受信された動画像データに含まれる利用許可情報と、前記入力手段により入力された文字・記号とを比較する比較手段と、前記比較手段による比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生手段により再生された始めの画像データから、前記動画像データを再度再生するように指示する指示信号を、前記外部情報処理装置へと送信する送信手段とを具備する装置として動作させることを特徴とする記憶媒体。

【請求項 24】 装置が実行可能なプログラムを格納する記憶媒体であって、前記プログラムを実行する装置を、出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信手段と、前記受信手段により受信された動画像データを前記複数のオブジェクトデータの各々に分離する分離手段と、前記分離手段により分離されたオブジェクトデータのうちの、利用許可情報を含まないオブジェクトデータを再生する再生手段と、文字・記号を入力する入力手段と、前記分離手段により分離されたオブジェクトデータのう

ち、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、前記入力手段により入力された文字・記号とを比較する比較手段と、

前記比較手段による比較の結果、前記利用許可情報と前記文字・記号とが一致した場合に、前記再生手段により再生された始めの画像データから、前記動画データを再度再生するように指示する指示信号を、前記動画データを構成する複数のオブジェクトデータに含まれる出所情報に対応する外部情報処理装置へと送信する送信手段とを具備する装置として動作させることを特徴とする記憶媒体。

【請求項25】 出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離手段と、前記分離手段により分離された複数の出所情報を管理する管理手段と、前記管理手段により管理される任意の出所情報により特定されるネットワーク上の情報機器に対して認証信号を送信する送信手段と、前記送信手段により送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信手段と、前記受信手段により受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御手段と、を具備することを特徴とする認証装置。

【請求項26】 前記出所情報は、URL (Uniform Resource Locator) の情報であることを特徴とする請求項25に記載の認証装置。

【請求項27】 前記複数のオブジェクトデータから構成される画像データは、圧縮符号化された動画データであることを特徴とする請求項25に記載の認証装置。

【請求項28】 前記管理手段により管理される任意の出所情報を選択する選択手段を更に具備することを特徴とする請求項25に記載の認証装置。

【請求項29】 前記送信手段は、通常、前記複数のオブジェクトデータから構成される画像データの受信用を使用されるインターフェースを、通常、方向に使用して前記画像データを受信する他、前記インターフェースを通常、方向と逆方向に使用して前記認証信号を送信することを特徴とする請求項25に記載の認証装置。

【請求項30】 前記送信手段は、MPEG4のビットストリームのアップストリームを使用して、前記認証信号を送信することを特徴とする請求項25に記載の認証装置。

【請求項31】 通信回線と接続するインターフェースを更に具備し、前記送信手段は、前記インターフェース及び前記通信回線を介して、前記情報機器に対して前記認証信号を送信し、

前記受信手段は、前記通信回線及び前記インターフェースを介して、前記情報機器から前記許可信号を受信する、

ことを特徴とする請求項25に記載の認証装置。

【請求項32】 出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離工程と、

前記分離工程で分離された複数の出所情報を管理する管理工程と、

前記管理工程で管理される任意の出所情報により特定されるネットワーク上の情報機器に対して認証信号を送信する送信工程と、

前記送信工程で送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信工程と、

前記受信工程で受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御工程と、

を含むことを特徴とする認証方法。

【請求項33】 各々ネットワークに接続して使用される情報機器と認証装置とを有する認証システムであって、前記認証装置が、

出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離手段と、

前記分離手段により分離された複数の出所情報を管理する管理手段と、

前記管理手段により管理される任意の出所情報により特定されるネットワーク上の前記情報機器に対して認証信号を送信する送信手段と、

前記送信手段により送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信手段と、

前記受信手段により受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御手段と、

を具備することを特徴とする認証システム。

【請求項34】 認証処理を制御するプログラムを格納した記憶媒体であって、該プログラムを読み込んで実行する装置を、

出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離手段と、

前記分離手段により分離された複数の出所情報を管理する管理手段と、

前記管理手段により管理される任意の出所情報により特定されるネットワーク上の情報機器に対して認証信号を送信する送信手段と、

前記送信手段により送信された認証信号に応答して前記

情報機器が送信した許可信号を受信する受信手段と、前記受信手段により受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御手段と、を具備する装置として動作させることを特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、認証装置及び認証方法及び認証システム並びに記憶媒体に係り、例えば、動画を再生する際に個々のオブジェクトに関して著作権保護等の目的で認証が必要となる場合に好適な認証装置及び認証方法及び認証システム並びに記憶媒体に関するものである。

【0002】

【従来の技術】図1は、従来のデジタル映像データの送受信システムを示す図である。図1に示すように、デジタル映像データの配信サーバー10は、それに付随したハードディスク等のデジタル映像データの記憶装置12に予め記録されているデジタル映像データを、デジタル映像データの受信クライアント20からの要求に応じてインターネット等のネットワーク網30を介して受信クライアント20にダウンロードする。ここで、配信サーバー10は、デジタル映像データを符号化する変換部11を有し、この変換部11によりデジタル映像データを符号化してデータ量を削減し、これをTCP/IPプロトコル等の手順に従って受信クライアント20に配信する。受信クライアント20側は、デジタル映像データを復号する変換部21を有し、この変換部21により受信に係るデジタル映像信号を再生し、表示、記録又は編集に供する。

【0003】1つの動画シーンを複数のオブジェクトで構成し、配信サーバー10の変換部11において各々のオブジェクトを符号化して圧縮し、これを受信クライアント20に転送し、受信クライアント20において、これらを復号し、再構成して動画シーンを再生するシステムの一例としてMPEG-4プレーヤーがある。

【0004】図2は、従来のMPEG-4プレーヤーの構成図である。図2は、「ISO/IEC FCD 14496-1 Fig. 1-1」に基づいて記載されたものであり、その詳しい説明については、「ISO/IEC FCD 14496-1」において述べられている。ここでは、その概略についてのみ説明する。

【0005】ネットワーク等を介して転送(transmission)されたMPEG-4ビットストリームやDVD-RAM等の記録メディア(storage medium)から読み出されたMPEG-4ビットストリームは、「TransMux Layer」において、転送/読み出しに相当する手順に従って受け取られ(sessionの確立)、「FlexMux」部に

おいて、シーン記述データ、オブジェクトデータ、オブジェクト記述データの各ストリームに分離し、復号し、再生され、シーン記述データ(scene description information)に基づいて、シーンが再生或いはグラフィック処理される。

【0006】なお、図3は、図2を模式化、簡略化したものである。ここで、個々のオブジェクトについて著作権保護等の目的で認証が必要となる場合、シーン記述データを含む複数のオブジェクトデータを含むビットストリームに「IP DataSet」(著作権情報群)を含ませることが考えられる。

【0007】

【発明が解決しようとする課題】しかしながら、転送ビットストリームに「IP DataSet」(著作権情報群)を含ませた場合でも、図2若しくは図3に示す構成では、仮に「Object Descriptors」において「IP Data」が再生されたとしても、画像の再生処理の際に「IP Data」についての処理がなされないため、「IP Protection」(著作権保護)処理が実行されることがない。

【0008】もちろん、この場合でもデコードされた「IP DataSet」をアプリケーションが受け取って「IP Protection」処理を実行することは可能であるが、この場合の処理はそのアプリケーションに固有の処理であり、他のプレーヤーや他の機種において同様の処理が実行されるとは限らない。

【0009】また、図2若しくは図3に示す構成では、個々のオブジェクトに対して認証処理を行った後に画像を再生するため、動画シーンを再生する際に次々と新しいオブジェクトが出現する場合には、その度に再生を一時的に停止して認証を求める必要があった。さらに、認証処理を行う際に、再生を停止しないでとくと、当然のことながら、認証処理にかかった時間分だけ、再生される映像が欠落してしまうという問題があった。

【0010】本発明は、上記の背景に鑑みてなされたものであり、例えば、認証処理を効率化し、著作権等の有効な保護と著作物の有効な利用を図るとともに、認証処理に関わる遅延時間により再生映像が欠落する問題を解消することを目的とする。

【0011】

【課題を解決するための手段】本発明の第1の側面に係る認証装置は、外部情報処理装置より利用許可情報を含む動画像データを受信する受信手段と、受信手段により受信された動画像データの一部を再生する再生手段と、文字・記号を入力する入力手段と、受信手段により受信された動画像データに含まれる利用許可情報と、入力手段により入力された文字・記号とを比較する比較手段と、比較手段による比較の結果、利用許可情報と文字・記号とが一致した場合に、再生手段により再生された始めの画像データから、動画像データを再度再生するよう

に指示する指示信号を、外部情報処理装置へと送信する送信手段とを具備したことを特徴とする。

【0012】上記の認証装置において、動画像データは、例えば、圧縮符号化された動画像データであることが好ましい。

【0013】上記の認証装置において、例えば、文字・記号をあらかじめ記憶した記憶手段を更に有し、比較手段は、例えば、受信手段により受信された動画像データに含まれる利用許可情報と、記憶手段に記憶された文字・記号とを比較することが好ましい。

【0014】上記の認証装置において、再生手段は、例えば、動画像データの時間的一部分若しくは空間的一部分を再生することが好ましい。

【0015】上記の認証装置において、送信手段は、例えば、指示信号と共に、当該認証装置が動画像データを利用可能であることを示す信号を送信することが好ましい。

【0016】上記の認証装置において、送信手段は、例えば、通常、動画像データの受信用に使用されるインターフェースを、通常、方向に使用して動画像データを受信する他、通常、方向と逆方向に使用して指示信号を送信することが好ましい。

【0017】上記の認証装置において、送信手段は、例えば、MPEG4のビットストリームのアップストリームを使用して、指示信号を送信することが好ましい。

【0018】上記の認証装置において、例えば、通信回線と接続するインターフェースを更に具備し、送信手段は、例えば、インターフェース及び通信回線を介して、指示信号を送信することが好ましい。

【0019】本発明の第2の側面に係る認証装置は、出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信手段と、受信手段により受信された動画像データを複数のオブジェクトデータの各々に分離する分離手段と、分離手段により分離されたオブジェクトデータのうち、利用許可情報を含まないオブジェクトデータを再生する再生手段と、文字・記号を入力する入力手段と、分離手段により分離されたオブジェクトデータのうち、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、入力手段により入力された文字・記号とを比較する比較手段と、比較手段による比較の結果、利用許可情報と文字・記号とが一致した場合に、再生手段により再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する外部情報処理装置へと送信する送信手段とを具備したことを特徴とする。

【0020】上記の認証装置において、出所情報は、例えば、URL (Uniform Resource Locator) の情報であることが好ましい。

【0021】本発明の第3の側面に係る認証方法は、外部情報処理方法より利用許可情報を含む動画像データを受信する受信ステップと、受信ステップにより受信された動画像データの一部を再生する再生ステップと、文字・記号を入力する入力ステップと、受信ステップにより受信された動画像データに含まれる利用許可情報と、入力ステップにより入力された文字・記号とを比較する比較ステップと、比較ステップによる比較の結果、利用許可情報と文字・記号とが一致した場合に、再生ステップにより再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、外部情報処理方法へと送信する送信ステップとを具備したことを特徴とする。

【0022】上記の認証方法において、動画像データは、例えば、圧縮符号化された動画像データであることが好ましい。

【0023】上記の認証方法において、例えば、文字・記号をあらかじめ記憶した記憶ステップを更に有し、比較ステップは、例えば、受信ステップにより受信された動画像データに含まれる利用許可情報と、記憶ステップに記憶された文字・記号とを比較することが好ましい。

【0024】上記の認証方法において、再生ステップは、例えば、動画像データの時間的一部分若しくは空間的一部分を再生することが好ましい。

【0025】上記の認証方法において、送信ステップは、例えば、指示信号と共に、当該認証方法が動画像データを利用可能であることを示す信号を送信することが好ましい。

【0026】上記の認証方法において、送信ステップは、例えば、通常、動画像データの受信用に使用されるインターフェースを、通常、方向に使用して動画像データを受信する他、通常、方向と逆方向に使用して指示信号を送信することが好ましい。上記の認証方法において、送信ステップは、例えば、MPEG4のビットストリームのアップストリームを使用して、指示信号を送信することが好ましい。

【0027】上記の認証方法において、例えば、通信回線と接続するインターフェースを更に具備し、送信ステップは、例えば、インターフェース及び通信回線を介して、指示信号を送信することが好ましい。

【0028】本発明の第4の側面に係る認証方法は、出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信ステップと、受信ステップにより受信された動画像データを複数のオブジェクトデータの各々に分離する分離ステップと、分離ステップにより分離されたオブジェクトデータのうち、利用許可情報を含まないオブジェクトデータを再生する再生ステップと、文字・記号を入力する入力ステップと、分離ステップにより分離されたオブジェクトデータのうち、利用許可情報を

含むオブジェクトデータに関して、当該利用許可情報と、入力ステップにより入力された文字・記号とを比較する比較ステップと、比較ステップによる比較の結果、利用許可情報と文字・記号とが一致した場合に、再生ステップにより再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する外部情報処理方法へと送信する送信ステップとを具備したことを特徴とする。上記の認証方法において、出所情報は、例えば、URL (Uniform Resource Locator) の情報であることが好ましい。

【0029】本発明の第5の側面に係る認証システムは、互いに通信可能に接続された情報処理装置と認証装置とを有する認証システムであって、認証装置が、情報処理装置から利用許可情報を含む動画像データを受信する受信手段と、受信手段により受信された動画像データの一部を再生する再生手段と、文字・記号を入力する入力手段と、受信手段により受信された動画像データに含まれる利用許可情報と、入力手段により入力された文字・記号とを比較する比較手段と、比較手段による比較の結果、利用許可情報と文字・記号とが一致した場合に、再生手段により再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、情報処理装置へと送信する送信手段とを具備したことを特徴とする。本発明の第6の側面に係る認証システムは、少なくとも1つの情報処理装置と、該情報処理装置と互いに通信可能に接続された認証装置とを有する認証システムであって、認証装置が、情報処理装置から出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信手段と、受信手段により受信された動画像データを複数のオブジェクトデータの各々に分離する分離手段と、分離手段により分離されたオブジェクトデータのうち、利用許可情報を含まないオブジェクトデータを再生する再生手段と、文字・記号を入力する入力手段と、分離手段により分離されたオブジェクトデータのうち、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、入力手段により入力された文字・記号とを比較する比較手段と、比較手段による比較の結果、利用許可情報と文字・記号とが一致した場合に、再生手段により再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する情報処理装置へと送信する送信手段とを具備したことを特徴とする。

【0030】本発明の第7の側面に係る記憶媒体は、装置が実行可能なプログラムを格納する記憶媒体であって、プログラムを実行する装置を、外部情報処理装置より利用許可情報を含む動画像データを受信する受信手段

と、受信手段により受信された動画像データの一部を再生する再生手段と、文字・記号を入力する入力手段と、受信手段により受信された動画像データに含まれる利用許可情報と、入力手段により入力された文字・記号とを比較する比較手段と、比較手段による比較の結果、利用許可情報と文字・記号とが一致した場合に、再生手段により再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、外部情報処理装置へと送信する送信手段とを具備する装置として動作させることを特徴とする。

【0031】本発明の第8の側面に係る記憶媒体は、装置が実行可能なプログラムを格納する記憶媒体であって、プログラムを実行する装置を、出所情報及び利用許可情報を含むオブジェクトデータを含む複数のオブジェクトデータから構成される動画像データを受信する受信手段と、受信手段により受信された動画像データを複数のオブジェクトデータの各々に分離する分離手段と、分離手段により分離されたオブジェクトデータのうち、利用許可情報を含まないオブジェクトデータを再生する再生手段と、文字・記号を入力する入力手段と、分離手段により分離されたオブジェクトデータのうち、利用許可情報を含むオブジェクトデータに関して、当該利用許可情報と、入力手段により入力された文字・記号とを比較する比較手段と、比較手段による比較の結果、利用許可情報と文字・記号とが一致した場合に、再生手段により再生された始めの画像データから、動画像データを再度再生するように指示する指示信号を、動画像データを構成する複数のオブジェクトデータに含まれる出所情報に対応する外部情報処理装置へと送信する送信手段とを具備する装置として動作させることを特徴とする。

【0032】本発明の第9の側面に係る認証装置は、出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離手段と、前記分離手段により分離された複数の出所情報を管理する管理手段と、前記管理手段により管理される任意の出所情報により特定されるネットワーク上の情報機器に対して認証信号を送信する送信手段と、前記送信手段により送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信手段と、前記受信手段により受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御手段とを具備することを特徴とする。

【0033】上記の認証装置において、前記出所情報は、例えばURL (Uniform Resource Locator) の情報であることが好ましい。

【0034】上記の認証装置において、前記複数のオブジェクトデータから構成される画像データは、例えば、圧縮符号化された動画データであることが好ましい。

【0035】上記の認証装置において、例えば、前記管

理手段により管理される任意の出所情報を選択する選択手段を更に具備することが好ましい。

【0036】上記の認証装置において、例えば、前記送信手段は、通常、前記複数のオブジェクトデータから構成される画像データの受信用に使用されるインターフェースを、通常、方向に使用して前記画像データを受信する他、前記インターフェースを通常、方向と逆方向に使用して前記認証信号を送信することが好ましい。

【0037】上記の認証装置において、前記送信手段は、例えば、MPEG4のビットストリームのアップストリームを使用して、前記認証信号を送信することが好ましい。

【0038】上記の認証装置において、通信回線と接続するインターフェースを更に具備し、前記送信手段は、前記インターフェース及び前記通信回線を介して、前記情報機器に対して前記認証信号を送信し、前記受信手段は、前記通信回線及び前記インターフェースを介して、前記情報機器から前記許可信号を受信することが好ましい。

【0039】本発明の第10の側面に係る認証方法は、出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離工程と、前記分離工程で分離された複数の出所情報を管理する管理工程と、前記管理工程で管理される任意の出所情報により特定されるネットワーク上の情報機器に対して認証信号を送信する送信工程と、前記送信工程で送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信工程と、前記受信工程で受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御工程とを含むことを特徴とする。

【0040】本発明の第11の側面に係る認証システムは、各々ネットワークに接続して使用される情報機器と認証装置とを有する認証システムであって、前記認証装置が、出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離手段と、前記分離手段により分離された複数の出所情報を管理する管理手段と、前記管理手段により管理される任意の出所情報により特定されるネットワーク上の前記情報機器に対して認証信号を送信する送信手段と、前記送信手段により送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信手段と、前記受信手段により受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御手段とを具備することを特徴とする。

【0041】本発明の第12の側面に係る記憶媒体は、認証処理を制御するプログラムを格納した記憶媒体であ

って、該プログラムを読み込んで実行する装置を、出所情報を含む複数のオブジェクトデータから構成される画像データを、前記複数のオブジェクトデータの各々と、該複数のオブジェクトデータの各々の出所情報とに分離する分離手段と、前記分離手段により分離された複数の出所情報を管理する管理手段と、前記管理手段により管理される任意の出所情報により特定されるネットワーク上の情報機器に対して認証信号を送信する送信手段と、前記送信手段により送信された認証信号に応答して前記情報機器が送信した許可信号を受信する受信手段と、前記受信手段により受信した許可信号に基づいて、前記任意の出所情報を含むオブジェクトデータを使用可能にする制御手段とを具備する装置として動作させることを特徴とする。

【0042】

【発明の実施の形態】以下、添付図面を参照しながら本発明の好適な実施の形態を説明する。以下の実施の形態は、所謂「back-channel」を利用して認証処理を効率化したシステムに関する。

【0043】（第1の実施形態）図4は、本発明の好適な実施の形態に係るMPEG-4プレーヤーを含むシステムの概略構成を示す図である。図4に示すシステムは、「IP Data Set」を操作して「IP Protection」を実現するシステムである。図4に示すシステムは、IPMPS（Intellectual Property Management and Protection System）207を有し、このIPMPS207により著作権認証及び保護機能を実現する点で図3に示すシステムと異なる。

【0044】図7は、認証処理に関するクライアントの動作を示すフローチャートである。以下、図7を参照しながら図4に示すシステムの動作を説明する。サーバー側では、マルチプレクサ201が、各々異なるURL（Uniform Resource Locator）としてURL1、URL2、URL3を持つ複数のネットワーク・サイト202～204から、夫々個々のオブジェクトを受信してこれらの複数のオブジェクトで構成される動画データを生成する。この動画データは、クライアントからの要求に応じてMPEG-4ビットストリーム205としてネットワークを介してクライアントに送信される。

【0045】ステップS1では、クライアントは、サーバーよりMPEG-4ビットストリーム205を受信する。このMPEG-4ビットストリームを構成する各オブジェクトには、著作権の帰属先を示す情報（ここでは、URLの情報）が付随している。ステップS2では、クライアントは、受信に係るMPEG-4ビットストリームをデマルチプレクサ206により複数のオブジェクトやそれに付随する情報（URLの情報を含む）等の複数のストリームに分離する。ここで、各オブジェク

トに付随するURLの情報は、「IP Data」のストリームである「IPMPS Stream」の一部としてIPMPS207に送られる。

【0046】ステップS3では、IPMPS207に送られた1又は複数のURLの情報の中から、いずれか1つのURLの情報を選択する。これは、例えば、操作者が指定するものであっても構わないし、所定の順序に従ってIPMPS207が選択しても構わない。

【0047】ステップS4では、選択したURLの情報に基づいて、ネットワーク上に接続された1又は複数のサーバのうち対応するURLを持つサーバ201に対して認証依頼信号を送信する。この場合、その送信には、後述するバックチャネル(back-channel)1又はバックチャネル(back-channel)2が使用される。

【0048】ステップS5では、認証依頼信号を受け取ったサーバ201からアクセス許可信号が送信されてくるのを待ち、アクセス許可信号を受信した場合はステップS6に進み、所定時間内にアクセス許可信号を受信しなかった場合はステップS7に進む。

【0049】ステップS6では、アクセス許可信号の受信によりアクセス許可(認証)が得られたオブジェクトに対するアクセスを可能にする。具体的には、アクセスコントロールポイントを制御する制御信号212を許可状態にすることにより、シーン・ディスクリプタ208、オーディオ・ビジュアル・デコーダ209、オブジェクトディスクリプタ210がデマルチプレクサ206の該当するストリーム(即ち、アクセス許可信号によりアクセスを許可されたオブジェクトのストリーム)にアクセスすることを可能にする。

【0050】一方、ステップS7では、アクセスコントロールポイントを制御する制御信号212を禁止状態にすることにより、シーン・ディスクリプタ208、オーディオ・ビジュアル・デコーダ209、オブジェクトディスクリプタ210がデマルチプレクサ206の該当するストリーム(即ち、認証を依頼したがアクセス許可が得られなかったオブジェクトのストリーム)にアクセスすることを禁止する。

【0051】ステップS8では、他のオブジェクトに付随するURLの情報があるか否かを確認し、当該URLの情報があればステップS3に戻り、なければ一連の処理を終了する。

【0052】シーン合成・グラフィック処理部211は、シーン・ディスクリプタ208、オーディオ・ビジュアル・デコーダ209、オブジェクトディスクリプタ210から供給されるデータに基づいて、シーン合成及びグラフィック処理を行う。この際、アクセス許可が得られたオブジェクトのみを再生の際の合成の対象としても良いし、1つでもアクセス許可が得られなかったオブジェクトがある場合に、一切の再生を行わないようにし

ても良い。

【0053】以下、上述した認証処理について更に詳細に説明する。

【0054】MPEG-4ビットストリームは、オブジェクト単位のビットストリームである「Elementary Stream」(ES)の内容を記述する「ES_Descriptor」と、オブジェクト自身を記述する「OD_Descriptor」を含む。ここで、「ES_Descriptor」或いは「OD_Descriptor」に、リモートアクセスのためのコマンドとアクセス先を指定するURLの情報が含まれている場合は、図5に示すような手順でリモートアクセスが実行される。

【0055】図5は、リモートアクセスを説明する簡略図である。図5において、「DAI」は、「DMIF Application Interface」と呼ばれる、MPEG-4ビットストリームとネットワークとのインターフェース層である。この詳細については、「ISO/IEC 14496-6 DMIFドキュメントDMIF Application Interface」の項に記載されているため、ここでは省略する。

【0056】また、MPEG-4ビットストリームは、「elementary stream」(ES)に対応したデコーダの種類についての情報を示す「DecoderConfigDescriptor」を含む。この「DecoderConfigDescriptor」は、幾つかのデータ要素の構造体であり、その中の要素の一つにストリーム型を示す1ビットのupStreamパラメータがある。この詳細については、「ISO/IEC 14496-1 FCD 8.3.4 DecoderConfigDescriptor」の項に記載されているため、ここでは省略する。

【0057】式1に、「DecoderConfigDescriptor」の一例を挙げる。

【0058】

[式1: DecoderConfigDescriptor]

```
aligned(8) class DecoderConfigDescriptor
{
    : bit(8) tag=DecoderConfigDescrTag {
        bit(8) length;
        bit(8) objectProfileIndication;
        bit(6) streamType;
        bit(1) upStream;
        const bit(1) reserved=1;
        bit(24) bufferSizeDB;
        bit(32) maxBitrate;
        bit(32) avgBitrate;
        DecoderSpecificInfo decSpecificInfo[];
    }
}
```

【0059】ここで、ストリームの識別は、式1の「D

「e」の値に基づいて行う。「streamType」の値は、表1のように定義されている。
 【0060】
 【表1】

表1: ストリーム型指定値

ストリーム型指定値	ストリーム型
0x00	reserved for ISO use
0x01	ObjectDescriptorStream
0x02	ClockReferenceStream
0x03	SceneDescriptionStream
0x04	VisualStream
0x05	AudioStream
0x06	MPEG7Stream
0x07-0x09	reserved for ISO use
0x0A	ObjectContentInfoStream
0x0B	IPMPStream
0x0C - 0x1F	reserved for ISO use
0x20 - 0x3F	user private

【0061】なお、表1は、「ISO/IEC 14496-1 FCD Table 0-1: streamType Values」に対して、この実施の形態に固有の「IPMPStream」を識別するための値を追加したものである。表1において、各パラメータや用語は、「ISO/IEC 14496-1 FCD」と同じであるので、ここでは説明を省略する。

【0062】図4に示すように、ストリームの向きを示すフラグである「DecoderConfigDescriptor.upStream」が「1」の時は、システムは、クライアント側からサーバ側にストリームを転送する「upstream」の状態になる。ここでは、この「upstream」の状態を利用した転送機能を「back-channel1」と呼ぶことにする。

【0063】通常の再生時は、「DecoderConfigDescriptor.upStream」

が「0」であり、サーバ側からクライアント側にストリームを転送する「downstream」の状態である。一方、オブジェクトに対するアクセスの許可を求める場合は、「DecoderConfigDescriptor.upStream」を「1」として、必要なデータをURL先へ「upstream」する所謂「back-channel1」を用いることにより、「IPMP Management Data」（著作権管理情報）を「IPMPStream」としてサーバ側に送り、リモートアクセスによりURL先から応答データを転送させることになる。

【0064】表1に示す「IPMPStream」は、「IPMP_ES」と「IPMP_D」の構成を有する。「IPMP_ES」の各々は一連の「IPMP_Messages」からなる。式2は「IPMP_Messages」の記述例である。

【0065】

```

[式2: IPMP_Message]
class IPMP_Message () {
    unsigned int(8)      IPMPS_TypeCount;
    bit(1)  hasURL;
    int i;
    for (i = 0; i < IPMPS_TypeCount; i++) {
        unsigned int(16) IPMPS_Type[[i]];
        unsigned int(32) offset[[i]];
        unsigned int(16) length[[i]];
    }
    if (hasURL) {
        unsigned int(5) lengthOfURLbits;
        bit(3) reserved=0b111;
        unsigned int(lengthOfURLbits) lengthOfURL;
        char(8) URLString[lengthOfURL];
    }
}

```

```

    }
    for (i = 0; i < IPMPS_TypeCount; i++) {
        char(8) IPMP_data[length[i]];
    }
}

```

【0066】式2において、「IPMPS_TypeCount」は、異なる「IPMPStype」の数を表わす。これにより、異なるIPMPSを存在させることが可能となるため、「IPMP messages」は複数のIPMPSに対応可能である。

【0067】なお、URLが指定されている場合は、「IPMPS_TypeCount」は0を取り、その他は最低値である1を取る。また、この場合、内部の「IPMP_Message」の代わりに、外部に格納されている「IPMP_Message」を参照して使用することになる。

【式3:IPMP_DescriptorUpdate】

```

aligned(8) class IPMP_DescriptorUpdate : uint(8) IPMP_DescriptorUpdateTag {
    unsigned int(8)    descriptorCount;
    int i;
    for (i = 0; i < descriptorCount; i++) {
        IPMP_Descriptor    d[[i]];
    }
}

```

【0070】式3において、「descriptorCount」は、更新される「IPMP_Descriptors」の数を表わし、また、d[i] は、ある一つの「IPMP_Descriptor」を表わす。式

【式4:IPMP_Descriptor】

```

class IPMP_Descriptor () {
    bit(8) IPMP_Descriptor_ID;
    unsigned int(8)    IPMPS_TypeCount;
    bit(1) hasURL;
    int i;
    for (i = 0; i < IPMPS_TypeCount; i++) {
        unsigned int(16)    IPMPS_Type[[i]];
        unsigned int(32) offset[[i]];
        unsigned int(16) length[[i]];
    }
    if (hasURL) {
        unsigned int(5) lengthOfURLbits;
        bit(3) reserved=0b111;
        unsigned int(lengthOfURLbits) lengthOfURL;
        char(8) URLString[lengthOfURL];
    }
    for (i = 0; i < IPMPS_TypeCount; i++) {
        char(8) IPMP_data[length[i]];
    }
}

```

【0068】また、「IPMPS_D」は、「IPMP Descriptor」からなる。この「IPMP Descriptor」は、個々の「elementary streams」に対する詳細なIPMP制御を行うためのデータ構造体である。そして、「IPMP Descriptor Updates」は、オブジェクト・ディスクリプタ・ストリーム（Object Descriptor stream）の一部として実行される。式3は、「IPMP Descriptor Updates」の記述例を示す。

【0069】

4は、「IPMP_Descriptor」の記述例を示す。

【0071】

【0072】式4において、「IPMP_Descriptor_ID」は、各「IPMP_Descriptor」に固有の番号であり、「ES_Descriptors」は、「IPMP_Descriptor_ID」を使って「IPMP_Descriptors」を参照する。また、「IPMPS_TypeCount」は、「IPMP_Message」で指定された異なるIPMPSの数を表わす。

【0073】図6は、URL先で更にURL指定がある場合の階層構造の例を示す図である。なお、図6は2階層の場合の例であるが、もちろん、更なるURL指定がある場合、3階層になっても4階層になってもよい。また、図6においては、「IPMPStream」を明示していないが、リモート指定されるオブジェクト(Object)に関する「IPMP_ES」か「IPMP_Descriptor」が、「SceneDescriptionStream」か「ObjectDescriptionStream」に呼応して、必要に応じデコードされ、リモートアクセスされることは、先に説明した図5の場合と同様である。

【0074】以上、MPEG-4のビットストリームの「upstream」の状態、即ち、バックチャネル(back-channel)1を使用した認証処理について説明したが、このような「back-channel1」を使用する認証処理は、リアルタイムのビットストリーム再生時における「upstream」処理であるので、比較的データ量が少なく処理時間の短い高速処理向けの場合を想定している。ここで、リアルタイム

再生をしているシステムでは、「back-channel1」によるリモートアクセス及び認証による遅延は極力少ないことが望ましい。

【0075】しかしながら、データ量が少ない場合であっても認証に相応の時間を要することがあり、その場合、「back-channel1」における遅延が問題となる。この場合、許容遅延時間の点、また、インタラクティブな操作性を必要とする点から考えると、第2の「back-channel」を設けることが好ましい。

【0076】そこで、この実施の形態では、MPEG-4のビットストリームを伝送するのとは異なるI/O(機器間入出力)インターフェースが設けられている。これを以下では「back-channel2」と呼ぶことにする。

【0077】まず、「back-channel2」を使用した認証処理を説明する前に、「back-channel1」と「back-channel2」におけるデータ量と遅延時間の関係を考える。「MPEG-4 Requirement Group」の報告では、リアルタイム再生を妨げない「back-channel1」の遅延許容時間は1フレーム時間とあるので、これに基づいて「back-channel1」と「back-channel2」における想定データ量と転送レートとの関係を求めると、表2のようになる。

【0078】

【表2】

表記	使用目的	データ量	遅延時間
back-channel 1	認証のための高速IPMP リモートアクセス	3000 - 5000 bits/s	100-300 ms
back-channel 2	認証のための低速IPMP 入出力アクセス		>500ms

表2 back-channel 1及び2の遅延時間とデータ量

【0079】ここで、認証のための高速IPMPリモートアクセスでは、100-500bit/Frame以内のデータ量を3K-5K/secの転送ラインで処理することが遅延時間の限界となる。「IPMP_Message」データや「IPMP_Descriptor」データとURL指定による「back-channel1」による「remote content access」の結果としてのdelay-bandwidthの関係を、表4と見ることができるので、実際の認証のためのデータ量は限られたものになる。一方、認証には、stream処理とは非同期に時間を要することが多い。

【0080】また、複数のオブジェクトの認証が一箇所のサイトではなく、複数のに跨ることも想定される。この場合には、表2の条件は更に厳しくなり、実用に耐えな

くなる。そのため、stream処理と非同期で低速処理が可能な認証手続きの場合には、「back-channel 2」を用いた方がよい。

【0081】以下、「back-channel 2」を使用した場合の処理について説明する。認証のための低速IPMP入出力アクセスのための「back-channel 2」は、図4に示すように、基本的にはMPEG-4ビットストリームを伝送するものとは異なるI/O(機器間入出力)インターフェースを対象としたものになる。

【0082】ここで、「back-channel 2」の先に、キーボードとディスプレイとモデムを有するコンピュータ端末214を用意し、電話回線とIPMPS 207とに接続する。この構成において、コンピュータ端末214は、認証の必要なストリーム中のオブジェク

トとその認証先の情報をIPMPS207から受け取り、その情報をディスプレイに表示する。操作者は、その表示を参照して、認証に必要なストリーム中のオブジェクトを選択する。コンピュータ端末214は、認証先に電話をかけて、認証方法やアクセスコードを該認証先から受け取り、その内容をディスプレイに表示する。操作者が、受け取った情報をキーボードを使って入力すると、その入力情報がIPMPS207に通知され、必要なオブジェクトに対するアクセスを許可状態にする。

【0083】ここでは、電話回線を利用する場合を例として挙げたが、この代わりに、例えば、CATVのケーブルや無線通信路を利用しても良い。

【0084】また、場合によっては、予め認証先との契約において入手したアクセス認証に必要な情報を格納したPC Cardをコンピュータ端末214内のPCMCIAインターフェースに差し込んで、アクセス認証に必要な情報をIPMPS207に通知して、オブジェクトに対するアクセスを許可状態にしてもよい。

【0085】なお、操作時間や認証時間がある程度長くなる認証処理の場合は、ストリーム再生の開始時やシーンチェンジ時等、リアルタイムでない場合に有効である。

【0086】このように、この実施の形態によれば、用途に応じて「back-channel1」又は「back-channel2」を選択して使用することができる。この選択は、操作者が行うことができるように構成してもよいし、システム内部で遅延時間限界等を考慮して最適な方を選択するようにしてもよい。

【0087】以上のように、2種類の異なる「back-channel」を設けることにより、柔軟性の高い認証処理を実現することができる。

【0088】（第2の実施形態）以上説明したように、第1の実施形態においては、当該MPEG-4プレーヤーが、ネットワーク上の接続された1又は複数のサーバのうち対応するURLを持つサーバに対して認証依頼信号を送信する際に、「back-channel」を用いる手法について説明したが、本第2の実施形態におい

ては、「back-channel」の他の利用方法について説明することにする。

【0089】図8は、図2、3に対して、著作権保護システム(IPMP System86)とオブジェクトデータ処理フロー制御部(IPMP Stream Flow Control83)とを加えたMPEG-4プレーヤーの概略図を示している。

【0090】図8は、図4における「アクセスコントロールポイント」におけるストリームの制御の内容を、より具体的に開示したものである。この図8において、著作権保護を要求する画像オブジェクト符号化データを含むMPEG-4ビットストリームはDemux Layer81で各々のオブジェクトデータに分割され、Sync Layer82で符号化やビットストリーム作成時に加えられた時刻刻印情報に従ってプレーヤー内部時間に変換・同期される。

【0091】一方、IPMP System86は、Demux Layer81で分離された著作権保護情報に基づき、個々に分離された著作権保護を要求するオブジェクトデータの認証処理を行い、IPMP Stream Flow Control83へ許可信号を渡してオブジェクトデータ処理フロー制御を行い、Compression Layer84にて、各オブジェクトデータは各オブジェクトデータ毎のデコーダで復号され、Composition Layer85にて、復号されたシーン記述にしたがってシーン合成を行い、表示する。

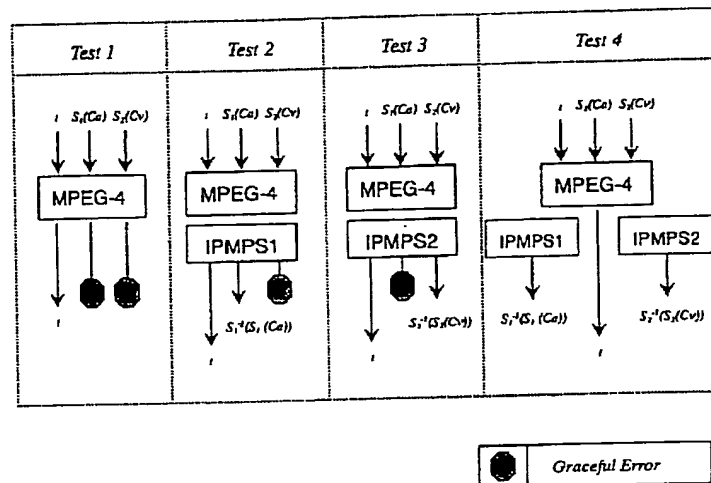
【0092】特に、オブジェクトデータ処理フロー制御の方法には、幾つかの方法が考えられ、ここでは例として、Test Condition #1と#2の2つを挙げて、解決しようとする問題の説明をする。

【0093】表3は、IPMP System(IPMPS)とStream FlowControlの関係を示す例として、4つのテストプランを示した図である。

【0094】

【表3】

IPMP Test Plan



【0095】この表3において、テスト1は、IPMP Systemが存在しない場合、テスト2は、IPMPS1だけが存在する場合、テスト3は、IPMPS2だけが存在する場合、テスト4は、IPMPS1とIPMPS2の両方が存在する場合を示している。

【0096】次に、各テストにおいて入出力する信号、及び、IPMPS1とIPMPS2の役割の違いについて説明する。まず、表3では、Unprotected Text Object Streamを“t”と表現し、Protected Audio Streamを“ $S_1(Ca)$ ”と表現し、Protected Video Streamを“ $S_2(Cv)$ ”と表現している。そして、 $S_1(Ca)$ 用IPMP Systemを“IPMPS1”と表現し、オリジナルの符号化データとASCII code “x”とのXOR（論理的排他和）の結果を“ $S_1(Ca)$ ”としている。従って解読キーはASCII code “x”で、出力は、オリジナルの符号化データと“x”との“XOR”となる。

【0097】また、 $S_2(Cv)$ 用IPMP Systemを“IPMPS2”と表現し、オリジナルの符号化

データとASCII code “a”とのXORの結果を“ $S_2(Cv)$ ”としている。従って解読キーはASCII code “a”で、出力は、オリジナルの符号化データと“a”との“XOR”となる。なお、“Graceful Error”とは、protected object streamを正常にキーで解読できなかったために起こるデコーダ以降でのエラーで、いわゆる“fatal error（致命的システムエラー）”ではなく、例えば、Protected Video Streamの場合の考えられる“Graceful Error”は、「表示されない」、若しくは、「乱れた画面が表示される」等のエラーである。テスト4の場合のみ、“Graceful Error”が発生しない。

【0098】表4は、IPMPのVerificationテストのコンディションとパラメータを示した図である。

【0099】

【表4】

IPMP Verification Test Condition and Parameters

Condition		Test 1	Test 2	Test 3	Test 4
Contents	α	Unprotected Text	<---	<---	<---
	S1(Ca)	Protected Audio	<---	<---	<---
	S2(Cv)	Protected Video	<---	<---	<---
IPMP Condition	IPMP-ES and IPMP-D	yes	yes	yes	yes
	IP Identification Data Set	yes	yes	yes	yes
	IPMP-S 1	none	XOR 'x' for S1(Ca)	none	XOR 'x' for S1(Ca)
	IPMP-S 2	none	none	XOR 'a' for S2(Cv)	XOR 'a' for S2(Cv)
Test Condition	#1	none	Embedded 'key' & constant delay	<---	<---
	#2	none	User interaction & non-fixed delay	<---	<---
	Synchronization	yes	yes	yes	yes
Expected result		α ; pass S1(Ca); error S2(Cv); error	α ; pass S1(Ca); pass S2(Cv); error	α ; pass S1(Ca); error S2(Cv); pass	α ; pass S1(Ca); pass S2(Cv); pass

【0100】この表4において、テスト2を実行する場合、Test Condition #1では、各オブジェクトストリームにとって正常なキーが、あらかじめIPMP System (IPMPS1, IPMPS2) に在り、入ってきたオブジェクトストリームを直ちに(また、一定の遅延時間で)「解読」して各デコーダに出力する。

【0101】また、テスト2を実行する場合、Test Condition #2では、各オブジェクトストリームにとって正常なキーが、あらかじめIPMP System (IPMPS1, IPMPS2) にはなく、外部からのキー入力やスマートカード挿入等のユーザーインタラクティブな方法によって正常なキーを入力し、入ってきたオブジェクトストリームを「解読」して各デコーダに出力する。そのため、遅延時間は一定ではない。

【0102】図9は、MPEG-4 System Playerの一例の内部機能ブロックダイアグラムとデータの流れを示した図である。この図9は、同期メカニズムの説明のために、実際のシステムを簡略化して示したものであり、IPMP Systemとオブジェクトデータ処理フロー制御は省略してある。

【0103】まず、アプリケーションから起動されるMPEG-4 System Playerの入り口関数、Execute()は、各機能モジュールを呼び起こし、データ領域バッファ確保や各機能関数へのメモリ割付などを行い、データ処理の準備をする。DMIF layerのService module関数としてのFlexDemux91によって、入力されるMPEG-4ビットストリーム、即ち、ネットワークからのパケットデータやデータファイルは、一連のデータ群として受け取られ、ALManager92へと渡される。

【0104】次に、ALManager92内部で、データ群から各オブジェクトデータ、例えば、ビデオデー

タ、オーディオデータ、シーン記述データ等のデータの分割され、各データチャネルとなってシーン記述やオブジェクト関連情報データは、BIFSDecoder93へ、ビデオ、オーディオデータはDecoder94へ渡される。

【0105】BIFSDecoder93及びDecoder94で復号されたシーン記述情報と、ビットストリーム作成時に加えられた時刻印情報に応じて、Presenter95やMedia Streamデータ処理部(不図示)で、各復号Media Object data (Video, Audio data)の時間関係を調整し、同期を取り、シーン合成する。

【0106】図10は、上記一連のデータ処理プロセスを簡略化したものである。この図10において、FlexDemux91は、MPEG-4ビットストリームを受け取り、各オブジェクトデータ毎のelementary stream (ES)に分ける。そして、ALManager92は、各オブジェクトデータ毎のESをデコード単位に分割し、BIFSDecoder93及びDecoder94は、各オブジェクト毎の復号処理を行う。そして、各オブジェクトデータ毎の復号されたデータ群Media Streamが生成され、Presenter95は、Media Streamデータを扱うMediaStreamImp::Fetch()関数を用いて、個々のオブジェクトデータの時間調整を行い、各オブジェクトデータを1シーン毎に合成し、表示する。

【0107】図11は、時間調整のデータ処理例を示す図である。この図11を用いて、Presenter95における時間調整処理について詳しく説明する。まず、ステップS1101において、System Playerの現在時間に許容値を加え(→dwCurrentTime)、その値に基づいて、ステップS1102において、処理予定データ(AU)の刻印時間(Ti

meStamp)をSystem Player時間に換算し(→dwTime)、ステップS1104において、現在時間(dwCurrentTime)と処理予定データ(AU)の刻印時間(dwTime)とを比較する。処理予定データ(AU)の刻印時間(dwTime)が現在時間(dwCurrentTime)より後であれば、ステップS1106に進み、実際のシーン合成処理を行い、処理予定データ(AU)の刻印時間(dwTime)が現在時間(dwCurrentTime)より前であれば、シーン合成に不適(時間的にシーン合成時間に間に合わないデータと判断)として、ステップS1105に進み、次のデータ処理ブロック(AU)を処理対象にする。

【0108】図12は、図11に示した時間調整処理について、タイムチャートで時系列に示したものである。この図12において、Object stream(AU0)は、Arrival(AU0)の時点で、BIFSDecoder93若しくはDecoder94のDecoding Buffer1201へ届き、その後デコードされて、エンコード時に付加された刻印時間DTS(AU0)の時点で、Presenter95のComposition Memory1202へ送られ、シーン合成時間CTS(CU0)の時点から、シーン合成される。そして、続くObject stream(AU1)も同様に、DTS(AU1)の時点でDecoding Buffer1201からComposition Memory1202へと移され、CTS(CU1)からシーン合成される。

【0109】このように、図12を見れば、図11において、Decoding Buffer1201における時間DTSが、実際の現在時点dwCurrentTime以降として、Composition Memory1202における実際のシーン合成時間CTSへと調整されていることが分かる。

【0110】図13は、図10に示した処理フローにIPMP Systemでの処理を加えたものである。具体的には、以下のような処理を行う。FlexDemux91がMPEG-4ビットストリームを受け取り、各オブジェクトデータ毎のElementary Stream(ES)に分け、ALManager92が各オブジェクトデータ毎のESをデコード単位に分割するところまでは、図10と同様である。そして、次に、ALManager92で分けられたオブジェクトデータから、特にIPMP関連情報に基づいて、protected streamを特定し、正常キーの入力・認証等のIPMP System処理を行う。そして、BIFSDecoder93及びDecoder94が、各オブジェクトデータ毎のデコードするデータ群であるMediaStreamを復号処理して、Presenter95が、個々のオブジェクトの時間調整を行い、1シ

ーン毎に合成し表示する。

【0111】ここで、一例として、表4に示したテスト2を実行した場合におけるTest Condition #1と#2のオブジェクトデータ処理フロー制御について説明する。まず、Test Condition #1の方法では、キー解読の時間は各IPMP System毎に一定の遅延としてデコーダへ伝えられるので、図8のComposition Layer84や、図9のPresenter95で吸収される範囲であるように全体の遅延を見込んでおけば、結果として同期の問題は起こらない。

【0112】一方、Test Condition #2の方法では、以下ようになる。図14は、テスト2をTest Condition #2で実行する場合のIPMP Systemの処理を説明したフローチャートである。まず、ステップS1401において、ALManager92でデコード単位に分割された各オブジェクト毎のストリームを得る。そして、ステップS1402において、正当なキー入力があったか否かを判別する。そして、正当なキー入力ではなかった場合は、ステップS1403に進み、protected streamの解読をしないで、HOLDする。また、正当なキー入力があった場合は、ステップS1404に進み、protected streamの解読を行い、次の処理へと進む。

【0113】テスト2をTest Condition #2で実行する場合に、図14に示したフロー制御が行われる場合には、正常なキー入力があるまでのストリームはsuspendされ、一方、non-protected streamや他の既に正常なキー入力によって認証・解読されたストリームは次のデコーダ処理、シーン合成のための時間同期処理へと移行する。この際、先のsuspend streamが正常なキー入力によって認証・解読され、次の処理へ移行するまでの経過時間は、各protected streamへのユーザーインタラクティブな操作のために、各々一定ではなく、また処理再開時点では、すでにdwTimeがdwCurrentTimeを過ぎていることも考えられる。

【0114】この場合、図11及び図12から明らかにように、再開されたストリームは少なくとも再開以降のdwTimeがdwCurrentTimeより後となるまでデコードされず、次の処理予定データ(AU)までスキップし(即ち、データが間引かれ)、スキップされた部分については、シーン合成されることはない。このように、Test Condition #2の方法では、一部のデータが間引かれてしまい、連続するコンテンツを最初から得ることができなくなる。

【0115】もちろん、有料放送のような"push"型のデータ配信では、基本的に時間帯に応じた片方向デ

ータ配信で、セットトップボックス等の認証機能付き受信システムでデータを受けるので、Test Condition #1で十分対応できるため問題はない。

【0116】しかしながら、例えば、視聴者が、インターネット上ホームページの、ある映画などの映像の初めの数分間のコマーシャルデモコンテンツ群を見て、その中から1つのコンテンツを選択して、課金認証後に、その映像を初めから入手・鑑賞したいような場合は、Test Condition #1では無論対応できないし、Test Condition #2では選択・認証後に再生を再開するため、視聴者は、それ迄に流れてしまったコンテンツを得ることができない。

【0117】また、MPEG-4では、ビデオオブジェクト毎の選択・再生が可能なので、先のコマーシャルデモコンテンツにおいては、認証処理されていない状態でも、人物や背景など、一部のオブジェクトだけをprotected streamとしてgraceful errorとして再生させ続けることが可能であるが、この場合でも、Test Condition #2では、選択・認証後に再生を再開するため、視聴者は、それ迄に流れてしまった正常かつ完全なフルコンテンツを得ることができない。このように、視聴者が、最初から完全なコンテンツを見たいと思った場合には、コンテンツ配信側のサーバに、最初から映像を再送するように指示する必要がある。

【0118】一般的な解決方法の一つは、選択・認証後の映像再生の再開時に、クライアント（ユーザ）側からサーバ（コンテンツ配信）側へとフルコンテンツの再送要求をすることであるが、通常、この要求を行うためには、サーバ側がクライアント側からの要求を受け取るために、サーバ側がクライアント側へ予めアプリケーションを提供しておく必要がある。

【0119】しかしながら、MPEG-4などのように複数のビデオオブジェクトコンテンツやオーディオオブジェクトコンテンツを各々異なるURL（Uniform Resource Locator）先から得てシーン合成する場合は、複数のコンテンツ配信のサーバの夫々に対するアプリケーションと認証・再送方法が必要となるので、プログラム管理が煩雑となり、方法としては現実的ではない。

【0120】そこで、本第2の実施形態では、そのような、最初から映像を再送するように指示する信号を、その要求先のサーバのURLの情報と、認証結果を示す情報とともに、第1の実施形態で説明した「back-channel」（「back-channel1」または「back-channel2」）を使用して、コンテンツ配信元のサーバへと送信するのである。

【0121】より具体的には、本第2の実施形態においては、通常の使用ではMPEG-4ビットストリームを受け取ってシーン再生処理する（downstream

処理する）プレーヤー側から、MPEG-4でのback channel機能を使って、プレーヤー側からサーバ側へと情報を配信する（即ち、図1に示したようなUpchannel informationで、認証・再送情報をUpstream処理する）ことで、各コンテンツ配信元サーバ側では、認証・再送情報の通信に関する部分を、IPMP System Interfaceと共に共有することとなり、プログラム管理の煩雑さを軽減することができる。

【0122】このように、第2の実施形態によれば、認証処理後に、ネットワークを介して著作物の再送要求を行うことが容易にできるので、認証処理に関わる遅延時間によって、再生される映像が欠落するといったことがなくなる。

【0123】なお、第2の実施形態においては、認証処理の方法については、特に問わない。即ち、第1の実施形態のように、ネットワークを介して各コンテンツ配信サーバに対して認証依頼信号を送って、該各コンテンツ配信サーバからアクセス許可をもらうのもよいし、また、MPEG-4プレーヤーの方に、予め正当なキーが記憶されていて、視聴者がローカルに認証作業を行うようにするのも構わない。

【0124】なお、本発明は、複数の機器から構成されるシステムに適用しても、一つの機器からなる装置に適用してもよい。

【0125】また、上記の実施の形態に係る装置又は方法を構成する構成要素の全体のうち一部の構成要素で構成される装置又は方法も、本件出願に係る発明者が意図した発明である。

【0126】また、上記の実施の形態に係る装置の機能は、プログラムコードを記録した記憶媒体をシステム或いは装置に固定的又は一時的に組み込み、そのシステム或いは装置のコンピュータ（又はCPU若しくはMPU）が該記憶媒体に格納されたプログラムコードを読み出して実行することによっても達成される。ここで、該記憶媒体から読み出されたプログラムコード自体或いは該記憶媒体自体が法上の発明を構成する。

【0127】プログラムコードを供給するための記憶媒体としては、例えば、フロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモ리카ード、ROM等が好適であるが、他のデバイスを採用することもできる。

【0128】また、コンピュータが記憶媒体から読み出したプログラムコードを実行することにより本発明の特有の機能が実現される場合のみならず、そのプログラムコードによる指示に基づいて、コンピュータ上で稼働しているOS（オペレーティングシステム）等が実際の処理の一部又は全部を負担する実施の態様も本発明の技術的範囲に属する。

【0129】さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備えられたメモリに書込まれた後に、そのプログラムコードの指示に基づいて、その機能拡張ボードや機能拡張ユニットに備えられたCPU等が実際の処理の一部又は全部を負担する実施の態様も本発明の技術的範囲に属する。

【0130】

【発明の効果】以上説明したように、本発明によれば、認証処理を効率化し、著作権等を有効に保護すると共に著作物等を有効に利用することができる。さらに本発明によれば、認証処理後に、ネットワークを介して著作物の再送要求を行うようにしたことにより、認証処理に関わる遅延時間による再生映像の欠落がなくなり、そのことにより、多くの認証処理方法が可能となる効果がある。

【0131】

【図面の簡単な説明】

【図1】従来のデジタル映像データの送受信システムを示す図である。

【図2】従来のMPEG-4プレーヤーの構成図である。

【図3】図2を模式化・簡略化した図である。

【図4】本発明の好適な実施の形態に係るback channelを行うMPEG-4プレーヤーの構成図である。

【図5】リモートアクセスを説明するための簡略図である。

【図6】URL先で更にURL指定がある場合の階層構造の例を示す図である。

【図7】認証処理に関するクライアントの動作を示すフローチャートである。

【図8】図3の構成にIPMP System処理部を追加した構成を示す図である。

【図9】MPEG-4プレーヤーの内部機能ブロックダイアグラムとデータの流れを示す図である。

【図10】図5におけるデータ処理プロセスを簡略化して示した図である。

【図11】MPEG-4オブジェクトアクセスデータユニットの時間調整動作例を示すフローチャートである。

【図12】Decoding BufferとComposition Memoryのデータ移動とタイミングを示す図である。

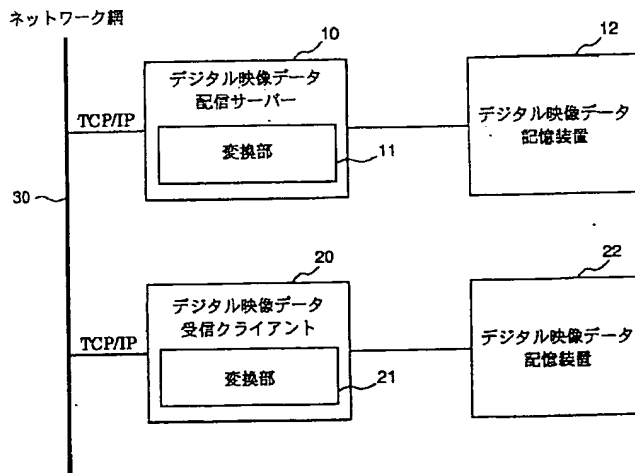
【図13】図6にIPMP System処理部を加えた場合のデータ処理プロセスを示す図である。

【図14】図8のIPMP Systemの動作例をしめすフローチャートである。

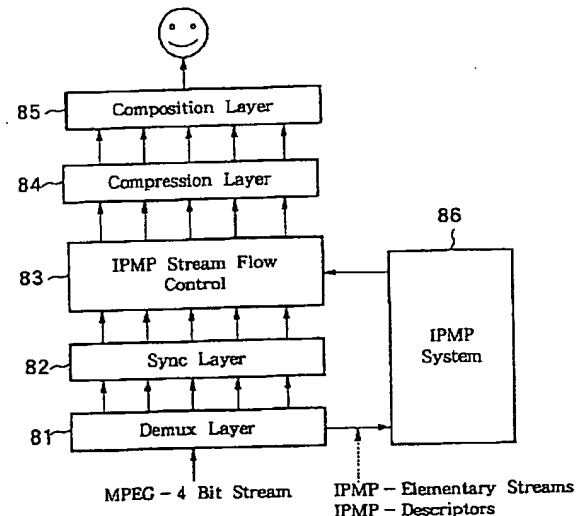
【符号の説明】

- 10 デジタル映像データ配信サーバー
- 11、21 変換部
- 12、22 デジタル映像データ記憶装置
- 20 デジタル映像データ受信クライアント
- 30 ネットワーク網
- 201 マルチプレクサ
- 202～204 ネットワーク・サイト
- 206 デマルチプレクサ
- 208 シーン・ディスクリプタ
- 209 オーディオ・ビジュアル・デコーダ
- 210 オブジェクトディスクリプタ

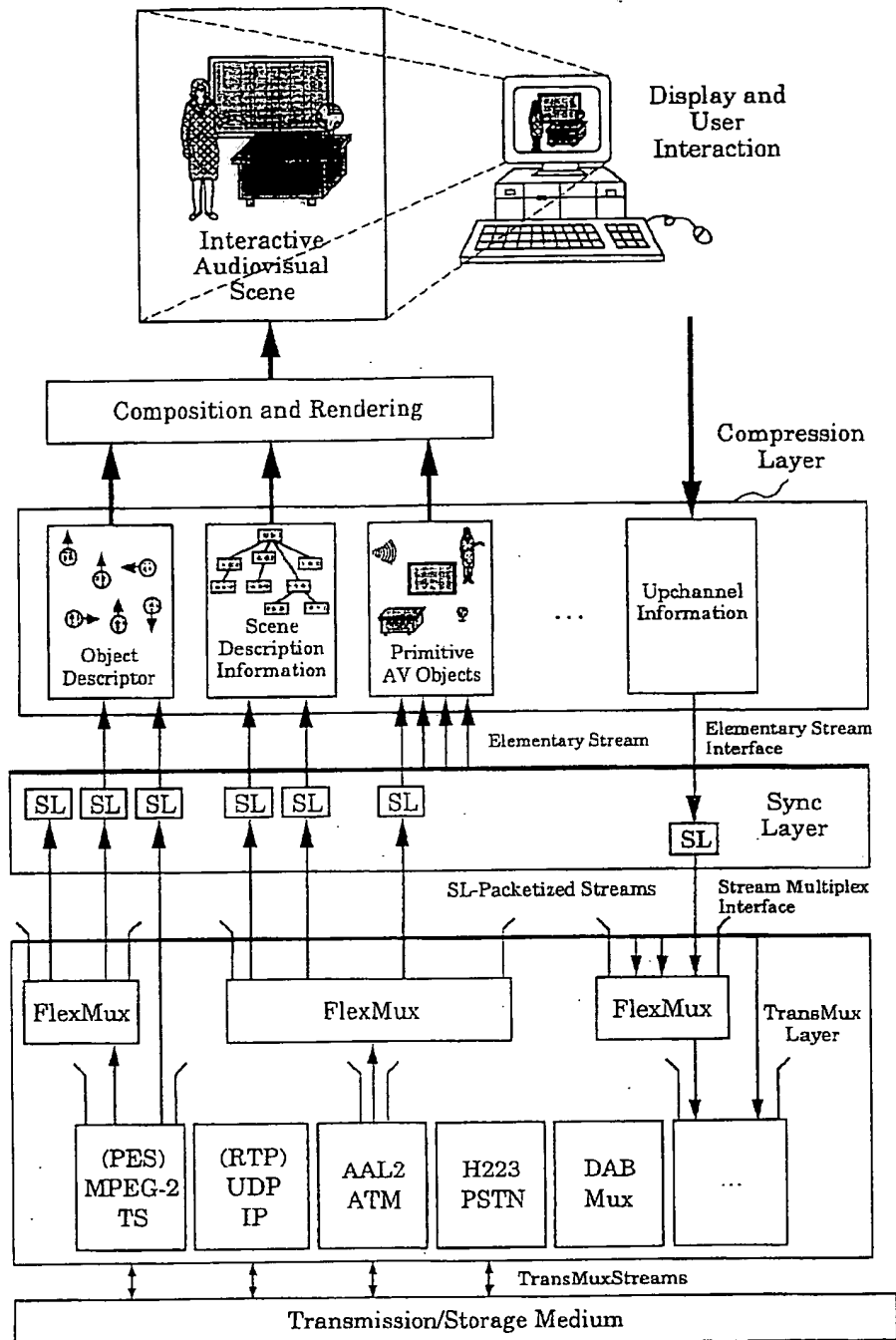
【図1】



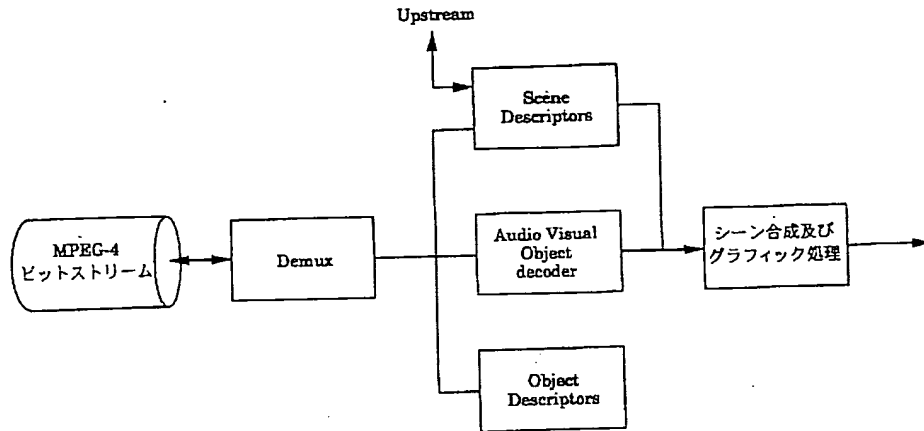
【図8】



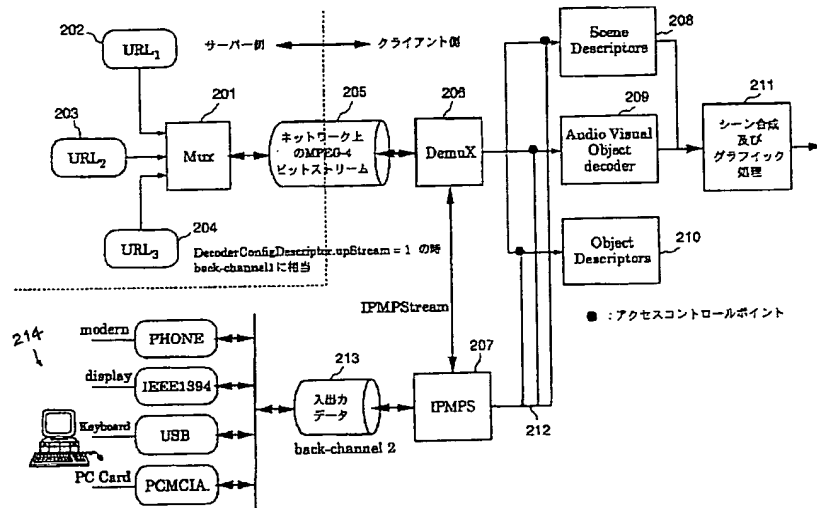
【図 2】



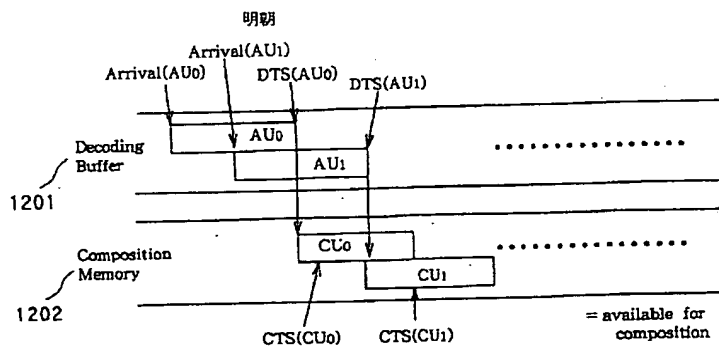
【図 3】



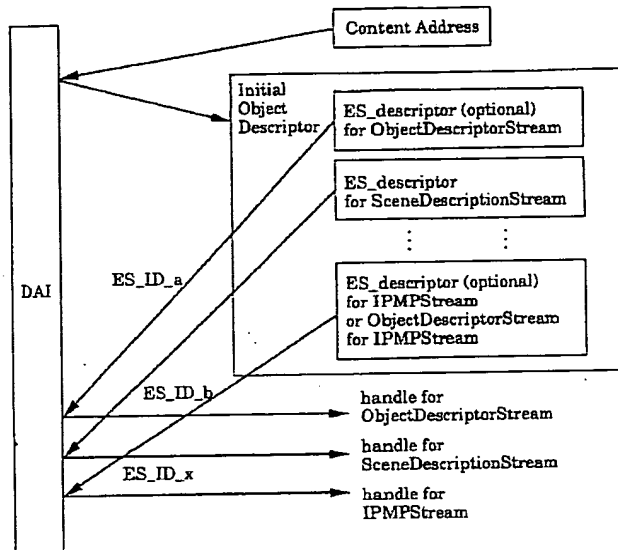
【図 4】



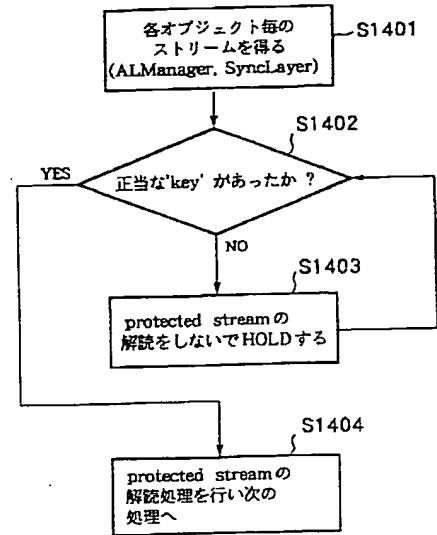
【図 12】



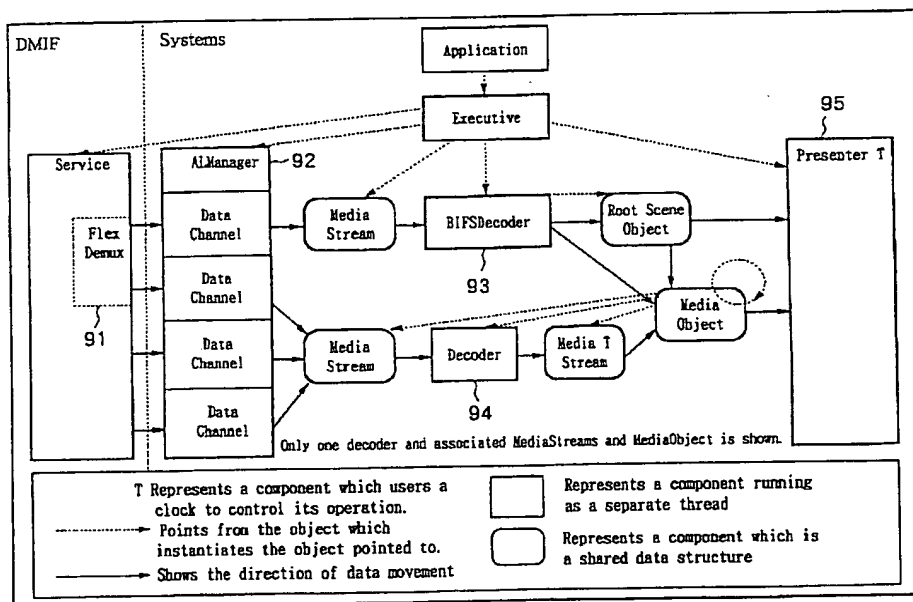
【図 5】



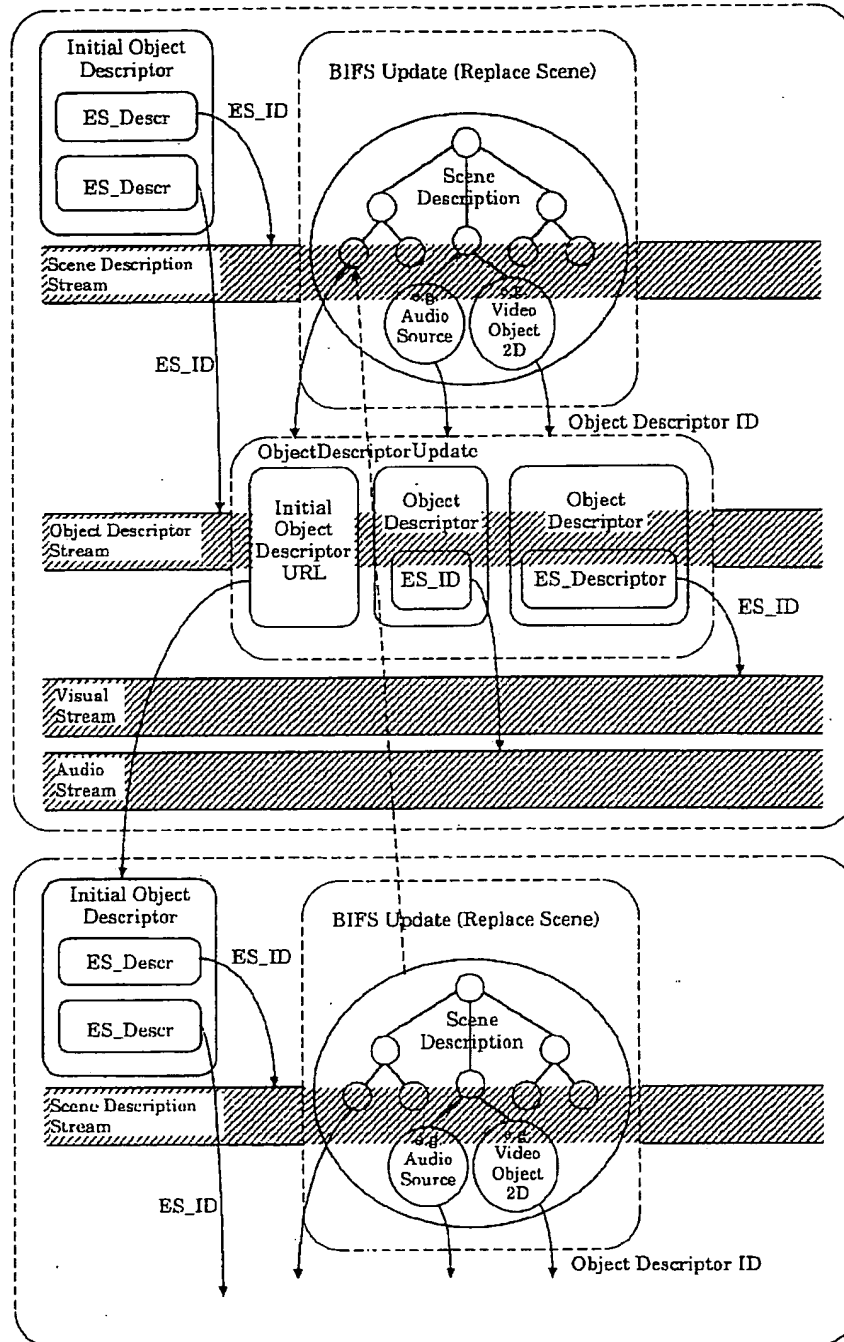
【図 14】



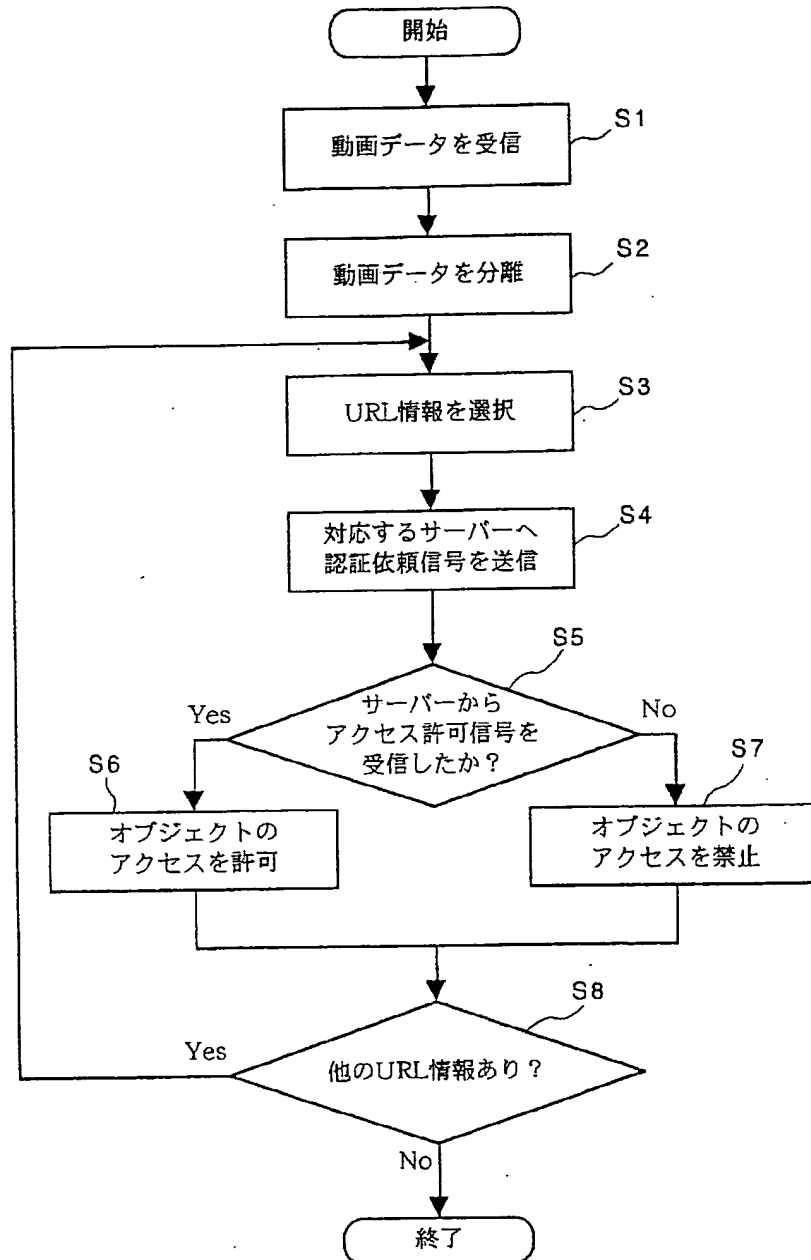
【図 9】



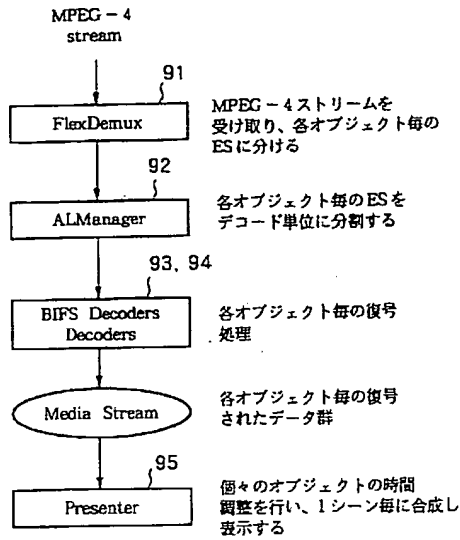
【図6】



【図7】

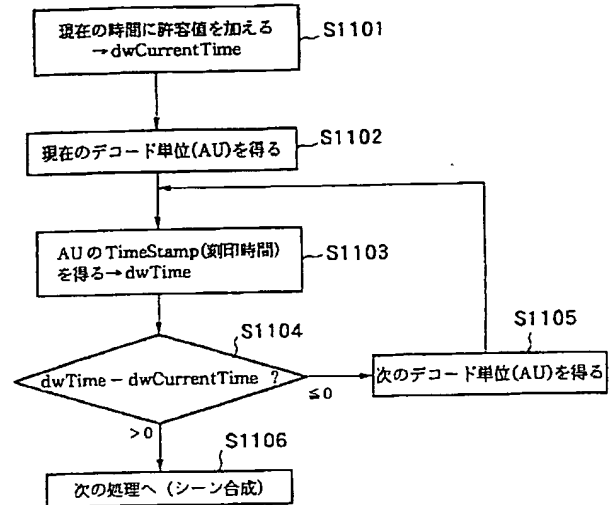


【図10】

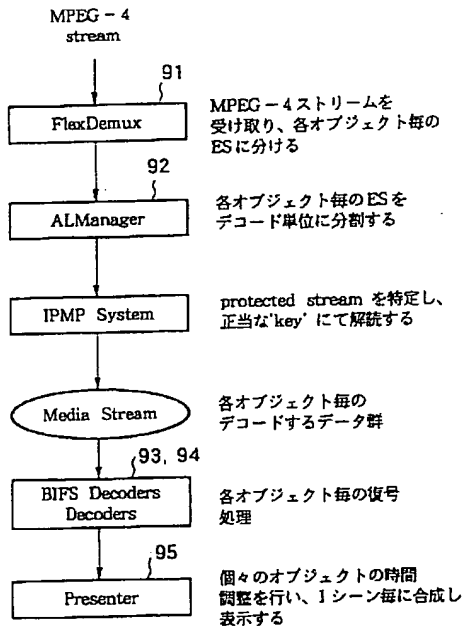


MediaStreamImp::Fetch0

【図11】



【図13】



フロントページの続き

(51) Int. Cl. 7

H 0 4 N 5/93

7/24

7/173

識別記号

6 1 0

F I

H 0 4 N 5/91

5/93

7/13

テマコード (参考)

P

E

Z